Chapter 8
The Essence of Cross-Domain Deterrence

Tim Sweijs and Samuel Zilincik

Contents

8.1 Introduction 130
8.2 The Origins of Cross-Domain Deterrence 131
8.3 The CDD Literature: Practical Innovation Versus Theoretical Reconceptualisation 133
8.3.1 Innovation in Practical Application 133
8.3.2 Attribution 134
8.3.3 Threat Credibility and Proportionality 137
8.3.4 Signalling 140
8.3.5 Escalation Management 142
8.4 Refinement and Reinterpretation—Expansion and Reconceptualisation 146
8.4.1 Refinement of Traditional Concepts of Deterrence 146
8.4.2 Reinterpretation of Deterrence by Denial 147
8.4.3 Expansion of Deterrence by Punishment: Norms, Delegitimisation and Entanglement 148
8.4.4 From Deterrence to Dissuasion 150
8.5 Conclusion 151
References 153

Tempora mutantur nos et mutamur in illis.

Abstract Both deterrence theory and deterrence practice are evolving to address contemporary strategic challenges. In the military domain, states progressively integrate and synchronise military operations. Outside of it, they exploit grey zone

T. Sweijs (✉)
The Hague Centre for Strategic Studies, The Hague, The Netherlands
e-mail: Timsweijs@hcss.nl

S. Zilincik
Masaryk University, Brno, Czech Republic
e-mail: zilinciks@gmail.com

F. Osinga and T. Sweijs (eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*, NL ARMS, https://doi.org/10.1007/978-94-6265-419-8_8

strategies that combine different instruments of influence across multiple domains. These developments are now giving birth to a new wave of thinking about cross domain deterrence (CDD), what it precisely entails, and what favouring conditions are necessary for it to be effective. This chapter situates CDD in the context of today's challenges, and identifies the prerequisites for these favouring conditions based on a review of a rather diverse body of literature. It finds that one strand of that literature predominantly focuses on practical and technical prerequisites in order for CDD to be effective, leaving the framework of traditional deterrence theory intact. It also finds a second strand that holds that the nature of today's challenges requires more than mere innovation in application. The ideas about deterrence proposed by this second strand are expanding on common understandings of deterrence to the extent that deterrence is no longer only about fear nor about convincing opponents to refrain from certain behaviour. The conclusion summarises the findings and elaborates their implications for theory and practice.

Keywords deterrence · dissuasion · cross domain · cyberspace · space · grey zone · hybrid threats

8.1 Introduction

Deterrence is about convincing adversaries to refrain from certain behaviour through the prospect of costs that outweigh the benefits.[1] As related in the preface to this volume by Osinga and Sweijs, deterrence has been a central tenet of strategic practice throughout history,[2] even if its logic was only clearly articulated in the aftermath of the Second World War. Deterrence scholarship has since then evolved in four consecutive waves. The first, second and third wave of the deterrence literature, which emerged during the Cold War, tended to almost exclusively focus on deterrence of high-intensity aggression including most importantly the possible use of nuclear weapons alongside large scale conventional invasion.[3] Lower-intensity threats which were considered mere nuisances were largely left outside of the scope of investigation.[4] However, these became more important in the 1990s with the demise of the Soviet Union and the emergence of non-traditional threats such as terrorism.[5] This gave birth to the fourth wave of deterrence literature that focused on the question whether deterrence would work against such threats that emerged in the 1990s and 2000s.[6] Over the past decade, a new body of ideas has been emerging concerning the application of deterrence in today's strategic

[1]Long 2008, pp. 7–8. See also the preface by Osinga and Sweijs in the present volume.
[2]Cioffi-Revilla 1999; Naroll 1974.
[3]Knopf 2010.
[4]Kennan 1948.
[5]Wilner 2011.
[6]Knopf 2010.

environment. An important characteristic of our age is the proliferation of ways and means by which hostile activities can be perpetrated. Accordingly, strategists have started to pay more attention to the application of deterrence in new domains and to cross domain deterrence (CDD), across both traditional and new domains. This chapter appraises the contribution of the emerging body of cross domain deterrence literature to deterrence theory and deterrence practice. It explains the context in which theories of cross domain deterrence have emerged and elaborates different conceptualisations of cross domain deterrence distinguishing between two different approaches. The conclusion summarises the findings and elaborates their implications for theory and practice.[7]

8.2 The Origins of Cross-Domain Deterrence

The shift in attention to CDD can be explained by two principal challenges. The first challenge relates to the progressive integration and synchronization of military operations across different domains (land, air, sea, cyber, and space) and the inherent disharmony between different levels of war (strategic, operational and tactical).[8] This is because military organizations aspire to better integrate physical, social and communication technologies in their ability to apply violence in the pursuit of political objectives, leading to strategic compression and cross domain warfare. Multi-domain operations concepts are being developed to guide efforts to synchronise actions both horizontally across domains and vertically across levels of war.[9] In light of the cross-domain nature of the challenge, strategists are envisaging analogous responses, including CDD.

The second challenge relates to the increased salience of "hybrid" or "grey zone" strategies that feature the simultaneous employment of military and non-military instruments, typically below the conventional military threshold, in an ambiguous fashion in order to evade attribution, with the goal to exploit adversary's vulnerabilities, in the pursuit of political objectives.[10] While the analytical value of the labels as such have caused considerable debate,[11] the real-world impact of these strategies poses a serious strategic challenge. Their increased salience stems from the enormous costs associated with interstate wars, which makes major military powers disinclined from waging actual hot wars against each other. These powers therefore try and find alternative ways to achieve their political objectives—in line

[7]This chapter builds on and further develops ideas that we first discussed in Sweijs and Zilincik 2019.

[8]Luttwak 2002.

[9]This is an evolutionary change, which has been long time in coming, and builds on earlier historical military strategic concepts such as Combined Arms Warfare, Joint Warfare, and Network Centric Warfare. See Black 2018; Johnson 2018; Hayes and Alberts 2003.

[10]Fridman 2018, p. 154; Morris et al. 2019, pp. 7–12; Hoffman 2018.

[11]See for example Stoker and Whiteside 2020.

with the original tenets of the coercive diplomacy literature. Furthermore, the increased salience of grey zone strategies also derives from the opportunities offered by new avenues to hurt opponents due to technological and societal developments because of the global wiring of societies over the past quarter century. Strategically innovative actors have been making frequent use of these avenues over the past decade to considerable effect. These developments have led scholars and strategists to start thinking about the use and utility of cross domain deterrence in dealing with adversaries employing cross domain strategies also outside the traditional military domains.

Authors from both sides of the Atlantic generally concur that cross-domain deterrence involves the use of threats in one domain to deter activities in (an)other domain(s). Some authors define cross domain deterrence exclusively in the military domains land, sea, air, cyber and space albeit at different levels of abstraction. James Scouras, Edward Smyth and Thomas Mahnken assert for example that it is the prospect of retaliation from one domain to another which constitutes the essence of CDD.[12] It is worth noting that the authors seem to focus exclusively on deterrence by punishment rather than denial. James Dawkins emphasizes that CDD involves the use of specific weapons rather than mere threats or retaliation in general. His conceptualization includes both punishment and denial strategies and draws attention to the actual instruments by which deterrent effects are to be achieved.[13] Despite the differences in abstraction, these authors understand CDD to operate specifically within the military domains.

Other authors also consider non-military domains and instruments. Accordingly, Manzo Vince understands CDD to refer to deterrent efforts on land, at sea, in the air, in space, in cyberspace and through economic sanctions as well as other non-violent instruments.[14] King Mallory, too, includes both non-military instruments and non-military domains, arguing that CDD is about preventing escalation in any domain and across them.[15] Sean Monaghan, Patrick Cullen and Njord Wegge assert that contemporary deterrence strategies should include an array of non-military means to detect, deter and respond in a tailored way.[16] More generically, Erik Gartzke and Jon R. Lindsay conceive of CDD as "the use of threats of one type, or some combination of different types, to dissuade a target from taking actions of another type to attempt to change the status quo".[17]

[12]Scouras et al. 2017.

[13]Dawkins 2009, p. 12.

[14]Vince 2015, p. 3.

[15]Mallory 2018, pp. 7–12. Vertical escalation, in the crisis escalation management literature, refers to escalating the intensity of force within one specific domain. Horizontal escalation refers to the expansion of escalation in other geographical domains, but can also describe escalation to non-traditional domains. For the original work, see Kahn 1965. For more recent elaborations on the concepts, see Morgan et al. 2008; Sweijs et al. 2016.

[16]Cullen and Wegge 2019.

[17]Lindsay and Gartzke 2019a, p. 4.

8.3 The CDD Literature: Practical Innovation Versus Theoretical Reconceptualisation

8.3.1 Innovation in Practical Application

Over the past decade or so, two approaches to CDD have emerged. The first approach emphasises that CDD requires merely the extension and refinement of the practical application of general deterrence theory. Authors within this approach argue that deterrence has always been cross domain in nature, albeit only in the context of traditional military domains.[18] Despite the emergence of new domains, deterrence in today's world is as such not different, so they argue.[19] Accordingly, Christopher Buckley asserts that cross domain deterrence has been practiced in the West for a very long time simply because "deterrence policy and strategy are concepts too big to be constrained in a single domain."[20] Still, it is acknowledged that particular aspects of deterrence in practice are in need of refinement. Gartzke and Lindsay, for example, observe that the "increasing complexity in the entire portfolio of means now available now appears to necessitate the refinement of deterrence as both a military and political process."[21] But what does refinement precisely entail for CDD to be effective? The authors in the refinement camp tend to focus on practical problems associated with the necessary conditions for effective CDD. Important requirements of deterrence in general that they focus on include attribution, threat credibility and proportionality, signalling and escalation management.[22] Attribution depends on the ability and the willingness to ascribe responsibility for a particular act to an actor. Without the possibility of attribution, transgressors can act undetected and therefore escape allocation of blame. Credibility is rooted in the perceived capability and willingness to act. It is crucial for deterrence to work because adversaries have to believe they will suffer negative consequences for their wrongdoings. Threats that are not credible are irrelevant for deterrence purposes. In general, threats which are proportional to their triggers are likely to be perceived more credible than disproportionate ones. Signalling refers to the process of communicating one's willingness and capabilities to act to instil that belief in the adversary. Attribution, credibility, threat proportionality and signalling together are prerequisites for escalation management, which is the regulation of the

[18]Mallory 2018, p. 6.

[19]Denning 2015.

[20]Buckley 2018.

[21]Lindsay and Gartzke 2016, p. 24. The quote is taken from the original draft of the chapter but it did not make it into the final version of the volume.

[22]George and Smoke 1974, p. 64; Long 2008, pp. 7–8.

intensity and scope of the conflict.[23] These four themes are given elaborate treatment in the CDD literature in the context of today's challenges.[24]

8.3.2 Attribution

CDD authors point out that the emergence of new domains and the proliferation of hostile actors complicates attribution in the cross-domain context. Both state and non-state actors can dispose of a range of military and non-military instruments to cause damage from afar. Geographic proximity is no longer required. Proxy wars have become increasingly salient, in the context of a steep increase in internationalized intrastate conflicts.[25] The democratization of the means of violence in combination with the foggy nature of new domains, especially cyber space, are singled out as formidable challenges to attribution in the cross domain context.[26] Special Forces and irregular combatants without uniforms, both of which are hard to identify, constitute key actors of choice to carry out contemporary military operations.[27] Low cost unmanned aerial vehicles enable conflict actors, including non-state actors such as ISIS in Iraq and Syria and the Houthis in Yemen, to target objects of value from a safe distance.[28] Individual grey zone events "are difficult to distinguish from one-off actions, statecraft, or diplomacy".[29] In the virtual realm, offenders can avoid attribution by hiding behind the anonymity provided by cyber space.[30] Though cyber attribution is possible in general, it is seldom certain in particular cases.[31] Perpetrators can exploit the complexity of cyberspace to pretend they act on behalf of a third party.[32] Furthermore, collecting sufficient evidence about the origins of cyber-attacks may take months.[33] By that time, too much time has passed for an effective response to effectuate deterrence.[34] Attribution in space brings its own set of challenges. The devices that scan the environment, those which keep track of space systems' health as well as those which identify the

[23]Morgan et al. 2008, p. 8.
[24]And in practical tabletop exercises, such as Wuest 2018.
[25]Innes 2012.
[26]Lehman 2019, p. 78.
[27]Cormac and Aldrich 2018, p. 479.
[28]Sayler 2015.
[29]Sheppard and Conklin 2019, p. 1.
[30]Nye 2017, pp. 49–52; Kello 2017, pp. 198–200.
[31]Klimburg 2017.
[32]Andres 2017, p. 94.
[33]Brantly 2018a, pp. 41, 45.
[34]Schneider 2019, pp. 105–6; Jackson 2019, p. 114.

origins of the hostile activities, have many blind spots.[35] Additionally, actors in possession of space assets will likely only know they have been attacked because of the effects of the attack. Also, space weather can produce damage akin to the adversarial action.[36] The origins of the attack and the identity of the perpetrator are therefore hard to pin down. The widespread use of non-military measures adds another layer of complexity to the attribution challenge. The different actors taking part in election meddling, disinformation campaigns, espionage, intelligence theft, critical infrastructure infiltration, political corruption or market stock manipulation may be hard to identify in acceptable time frames, or at all.[37] Overall, recent technological progress combined with the proliferation of actors and domains complicates attribution in both military and non-military domains and across them.

Yet, CDD scholars come up with various solutions to these obstacles to attribution which are first and foremost practical and technical rather than theoretical in nature. In general, the scholars acknowledge that the solutions to the attribution challenge across domains require international and inter-organizational cooperation, information sharing, technical expertise, analytical skills as well as political will. To deal with the hard-to-identify non-state actors and the wide spectrum of instruments at their disposal, it is suggested to attribute and threaten those upon whose help the non-state actors may be dependent. The assumption here is that these supporting actors are often states, which should render attribution easier.[38] In cyberspace, solutions are sought in the combination of technical, cognitive and behavioural expertise to help lift the fog of anonymity and enable effective responses.[39] It is argued that cross triangulation of the digital footprint, geographical origin, modus operandi, as well as geopolitical intent, renders attribution in cyber space in fact possible in the fast majority of cases.[40] Adversarial interest is also singled out as being particularly relevant in the attribution process.[41] Additionally, cyber-attacks intended to cause serious damage are more likely than not to be accompanied by non-cyber measures, which should also help identify the potential perpetrator.[42] Lack of political will may be a bigger obstacle than technical limitations. It is pointed out, for instance, that Obama's administration was well aware of the identity of the election meddling perpetrators in 2016 but nonetheless decided not to

[35]Suzuki 2018, p. 45.

[36]Harrison 2014, p. 117.

[37]See for example Treverton 2018.

[38]Mallory 2018, pp. 10–17.

[39]Iasiello 2014, p. 58.

[40]Valeriano and Maness 2015, p. 10. See the guide to cyber attribution specifying general indicators and examples of successful attribution by Office of the Director of National Intelligence 2018.

[41]Blagden 2020.

[42]Davis 2017, p. 80.

ascribe responsibility publicly so as to avoid further escalation.[43] It is also argued that the attribution problem can be bypassed by heavier reliance on deterrence by denial. Deterrence by denial in the cyber context can be further enhanced by military, political or economic measures to secure physical infrastructure and supply lines.[44] Attribution in the cyber domain is thus certainly more complex but authors argue that obstacles can be solved with the appropriate amount of expertise and will.

Myriad solutions to attribution problems in other domains are also proposed. In space, CDD authors focus not only on the hardening of satellite assets to bolster deterrence through denial; they also suggest the strengthening of situational awareness through monitoring capabilities that enable attribution; the assessment of geopolitical risk based on analysis of strategic intent and space capabilities; and the traditional exploitation of human intelligence sources.[45] In the terrestrial military domains, it is argued that attribution is progressively less of a problem. Attribution of actions executed by irregular forces can exploit data from social media, photos and position tracking applications.[46] Western countries were thus able to identify and attribute Russian troop movements near the Ukrainian border during the summer of 2014. Likewise, the US was able to quickly ascribe the 2019 hostile activities in the Persian Gulf to the Iranian Revolutionary Guards units.[47] North Korean missiles launches over the past decade were also time and again detected by US satellite systems.[48] Finally, attribution of actions outside these military domains can also be enhanced, it is suggested, by tracing overall patterns. Authors point out for instance that one diplomatic visit of a foreign official may not be significant, but when placed in a broader picture, and when combined with other actions, it may allow for the identification of an overall pattern of coercive activities.[49] On a more practical note, Linda Robinson et al. suggest that hybrid campaign analysis units that can expose systematic patterns and generate more holistic threat pictures, will contribute to cross domain attribution capabilities.[50] In sum, authors in the refinement strand suggest that attribution challenges can be addressed and overcome largely through the implementation of a series of practical recommendations.

[43]Healey 2018.

[44]Schneider 2019, pp. 112–113.

[45]Harrison 2014, p. 117; Kopec 2019, p. 123; Bahney et al. 2019, p. 139.

[46]Mallory 2018, p. 13.

[47]Yee et al. 2019.

[48]Wall 2019.

[49]Sheppard and Conklin 2019, p. 1.

[50]Robinson et al. 2018.

8.3.3 Threat Credibility and Proportionality

The issue of how to render deterrent threats credible in CDD is made more complicated by the inherent disproportionality of responses across domains and instruments of power.[51] In short, decision makers lack agreed-upon guidelines for proportional responses to the wide array of potential hostilities in CDD.[52] This is different from within-domain deterrence as Thomas Schelling's captured in his observation that "there is an idiom in this interaction, a tendency to keeps things in the same currency, to respond in the same language, to make the punishment fit the character of the crime."[53]

The conversion mechanism between violent and non-violent actions and their effects is seen as the biggest hurdle to threat proportionality.[54] Using violence against non-violent hostilities such as theft, espionage, infiltration or election meddling is likely to be seen as disproportionate by many. This is further exacerbated by the multitude of state and non-state actors, each of which may have different beliefs about the appropriate conversion ratio between violent and non-violent measures.[55] As one scholar puts it, "while the United States could threaten to retaliate against cyberattacks asymmetrically through economic sanctions or military threats, there is a significant chance that such actions would appear escalatory, disproportionate, or otherwise inappropriate to the American public or the international community."[56] Furthermore, actors operating through cyberspace are likely to have different degrees of tolerance for escalation risks because of their "anonymity, invulnerability, and global flexibility".[57] This exacerbates the proportionality asymmetry because it is not clear how individual actors and groups appraise the severity of cyberattacks. Moreover, retaliatory threats involving actions in cyberspace may have significant second and third order consequences. Their ultimate proportionality is thus hard to assess beforehand.[58] Additionally, propaganda, infiltration, espionage, economic sanctions and stock market manipulations tend to produce their effects slower than the implements of violence on land, on sea, in the air or in space.[59] Ultimately the conversion ratio between violent and non-violent measures is unclear because the former tend to have more direct and immediate effects while the latter tend to rely on more gradual and second order effects.

---

[51] See for instance Dawkins 2009, p. 12.
[52] Morrow 2019, pp. 187–188.
[53] Schelling 1966, pp. 146–149.
[54] Waxman 2013, pp. 111–113.
[55] Lewis 2010, pp. 2–3.
[56] Andres 2017, p. 96.
[57] Trujillo 2014, p. 49.
[58] Romanosky and Goldman 2016.
[59] Milevski 2019.

Even when it comes to conversion within single instruments of violence or against similar targets, proportionality assessments are not necessarily straightforward. For example, in space, the problem of proportionality is exacerbated by the differences in value which the individual actors tend to place on the same assets. The US is much more dependent than China on its satellites, both for military and civilian purposes. Therefore, the simple cost-benefit equation of destroying one satellite for each one destroyed by the enemy is asymmetric and therefore disproportional.[60] In fact, the costs incurred by the US are disproportionately higher.[61] It is argued that this undermines the credibility of US threats to harm space assets of states that do not rely on these systems in equal measure.[62] Finally, attacks against targets in and through new domains may cause considerable collateral damage which again further complicates proportionality assessments. For example, retaliation against space objects may cause debris which can threaten both friendly and hostile activities in outer space.[63] Alternatively, threatening terrestrial attacks in response to hostilities against satellites may be deemed disproportionate because the former may result in human casualties while the latter is likely to produce only material damage.[64] In this regard, authors point at patterns of failed deterrence when it comes to deterring less destructive hostilities.[65]

In tackling proportionality and credibility in CDD, scholars propose various solutions. In general, authors discuss strengthening cross domain deterrent postures by explicitly formulating cross domain threats in deterring domain specific actions, for instance by including conventional or even nuclear responses to enhance the credibility of threats seeking to deter attacks on critical assets in cyber space and space.[66] Some treatments suggest that a degree of proportionality can be established by focusing on the effects of specific actions rather than on the specific instruments used in this process.[67] Schneider, for example, speculates that cyber sabotage of a radar system can be countered proportionately by the electromagnetic jamming of a similar target. However, as she notes, this is likely to work better with direct, kinetic effects than with less direct, and less tangible effects. Smeets and Lin point out that states can build up credibility by regularly deploying a capability in practice. Actors with a clear track record of using particular capabilities, whether violent or not, may

[60]Lewis 2010, p. 3.
[61]Suzuki 2018, p. 46.
[62]Lambakis 2019, p. 503; Morgan 2010, p. xiii.
[63]Kopec 2019, pp. 125–126.
[64]Bahney et al. 2019, p. 140.
[65]Lewis 2013, p. 62.
[66]Lindsay 2015, p. 58.
[67]Manzo 2011, p. 7.

be able to develop sufficient reputation to offset the lack of credibility posed by the instruments themselves.[68]

CDD is seen as particularly relevant in the context of cyber deterrence. It is argued that cyber deterrence also requires a broad mix of military, diplomatic, economic and legal measures,[69] synchronised within an overall deterrence posture. To bolster credibility, "cyber deterrence needs to be a well-integrated defence component that is in tune with non-cyber policy initiatives, and to accomplish this, policymakers need to juxtapose carefully cyber deterrence means and ends to those involved in broader defence policies".[70] For the sake of credibility, cyber deterrence improvements need to be "mutually reinforcing", to have the potential to surprise the adversaries as well as to flexibly manoeuvre between both denial and punishment options. Furthermore, some argue that states are likely to consider truly destructive cyberattacks as regular acts of war, which should make threats of conventional military retaliation credible, as international law already allows such responses when the principles of necessity and proportionality are adhered to.[71]

Some scholars are also optimistic about the credibility of other non-violent measures. It is argued that election meddling too can be deterred by the threats of economic sanctions targeted against energy, banking and defence sectors.[72] Additionally, in response to serious threats posed by authoritarian governments, Western democracies can threaten to disrupt the former's protected information sphere and to leak sensitive information about the regime's misconduct to the foreign public.[73] Finally, as Jervis reminds us, it is necessary to realize that "threats need not be completely credible in order to be effective": it may be enough for threats to be probable rather than certain, no matter whether one employs violent or non-violent measures; "credibility is not an objective, nor is it a property of the person or state making the threat. Rather it is 'owned' by the target."[74] This underscores that conversion rates ultimately hinge on the perception of the beholder.

To deal with the proportionality issue as it relates to violent instruments, a generic solution that is proposed is to rely on a set of strategies to resolve the proportionality issue in different contexts. Anthony Juarez for instance lists counter-force, counter value, tit for tat, denial and ambiguity as potential options.[75] It is also argued that the supposed asymmetries in interests and values as related to space should not be overrated. For example, while some nations may not be as

[68]Smeets and Lin 2018, p. 63. Although the overall role of reputation is contested see for instance Mercer 1996; Press 2005.

[69]Wilner 2019, p. 9.

[70]Mandel 2017, p. 234.

[71]Davis 2017, p. 80.

[72]Wright 2019.

[73]Mallory 2018, p. 11.

[74]Jervis 2016, pp. 67–68.

[75]Juarez 2016, p. 6.

dependent on the satellites for their military utility, they may still value them highly for economic, cultural or prestige reasons and will therefore consider them vital assets.[76] With respect to the US it is said that it can credibly threaten retaliation against attacks aimed at its space assets everywhere precisely because its space assets are so important.[77] To deal with the disproportionality issue, it is recommended to focus on the overall effects rather than on specific instruments. In the context of space, this should involve a broad menu of "kinetic or non-kinetic attacks on adversary command, control, communication, intelligence, surveillance, and reconnaissance (C3ISR) and reconnaissance, surveillance, targeting, and attack (RSTA) assets in the land, air, and sea domains".[78] Overall, the recommendations from authors who are concerned with the effectuation of CDD in this refinement strand focus on establishing proportionality and increasing credibility through the adoption of a combination of these practical measures.

8.3.4 Signalling

Signalling in the cross-domain context is more complex for two reasons which are closely related to establishing proportionality. First, it is harder to relate signals about particular actions in one domain to anticipated reactions in another in line with Schelling's previously cited observation. Moreover, while signals relying on military instruments may resonate more than those relying on non-military instruments, they also come with higher risks of misunderstandings. For example, a signal of resolve to respond to cyberattacks by moving platforms for the launch of conventional or nuclear weapons may be easily interpreted as a preparation for hostilities rather than as an adjustment of the deterrence posture.[79] Conversely, signalling purely in cyber space may be difficult, because unlike in other domains, the relevant infrastructure of that domain is not under the exclusive control of the government.[80] Consequently, signals may get lost or be ignored by the adversaries.[81] Striking the right balance between over signalling on the one hand and under signalling on the other thus constitutes a paramount challenge to communication in the cross domain context. Second, a number of modern instruments and tactics are effective precisely because they are secret. This implies a serious trade-off for the signaller who runs the risk of losing the advantage yielded by the capability the moment it signals its possession. After all, it allows adversaries to devise effective countermeasures, which is especially pertinent in cyberspace, but

[76]Harrison 2014, p. 115.
[77]Buckley 2018.
[78]Mallory 2018, p. 10.
[79]Manzo 2015, p. 97.
[80]Rovner 2019.
[81]Iasiello 2014, p. 57; Valeriano and Maness 2015, p. 60.

also applies to hybrid operations.[82] This then raises the question of how to signal true capabilities while maintaining their utility for prospective hostilities.

CDD authors discuss an assortment of, once again, predominantly practical measures to meet these signalling challenges. For example, it is argued that the issue of tying threats across domains can be tackled by synchronized signalling at different levels of conflict. At the political level, signalling takes the form of public and private communication as well as norm development, at the strategic level it conveys the developments of doctrines about the actions and reactions, and at the tactical level it contains the actual application of particular forms of power to demonstrate resolve and capabilities.[83] The US successful orchestration of this kind of effort across different levels to signal its discontent with Chinese espionage activities during the Obama administration is a case in point.[84] To signal the relationship between different domains is thus possible but it requires the synergistic employment of communication across more levels than previously.

To tackle the issue of secrecy versus effectiveness, several suggestions are offered. One approach, which builds upon the recognition of the temporary nature of cyber capabilities noted by several scholars, may rely on building up a redundant portfolio of those capabilities, some of which can then be regularly used to demonstrate cyber capabilities.[85] The logic behind this option is that cyber weapons by their very nature are transitory—they lose their effectiveness over time because cyber vulnerabilities are exposed and patched.[86] Therefore, they can be disposed of for signalling both capability and resolve without losing their effectiveness. Other scholars suggest alternative ways that bypass the issue altogether by public advertisement of attribution technologies.[87] This way actors signal both their will and capabilities to allocate blame if necessary alongside announcement of the type of weapons and/or attacks they consider to be the most threatening. It is also argued that cyber weapons in fact possess signalling advantages compared to traditional instruments on the grounds that they can be used in a demonstration of force without starting the conflict they seek to prevent because they do not necessarily involve violent, kinetic effects.[88] That quality renders them sufficient to signal intent while avoiding escalation.[89] Additionally, states can rely on a combination of public speeches and real action to signal their cyber-capabilities. More states have been openly talking about the possession of sufficient cyber capabilities in recent

[82]Green and Long 2019, p. 206

[83]Sweijs and Zilincik 2019, p. 24.

[84]Brantly 2018a, pp. 18–19.

[85]Smeets 2017.

[86]Ablon and Bogart 2017.

[87]Lindsay 2015, p. 58.

[88]Lonsdale's argument does not go uncontested. See for example Stone 2013. Also, Lonsdale himself concedes that though non-violent in their nature, cyberattacks can produce violent consequences indirectly.

[89]Lonsdale 2018, p. 417; Schneider 2019, pp. 116–117.

years, some of whom have followed up with actions, such as Russia in Ukraine and the US in the context of its strategy of persistent engagement.[90] Some actors may be willing to signal more than others because of their strategic culture.[91] Signalling one's capabilities may even not inevitably lead to the loss of effectiveness, because not all adversaries are able or willing to patch the revealed vulnerabilities,[92] Moreover, cross domain signalling by military, political or economic measures may alleviate the problem with clandestine capabilities because conventional forces, diplomatic pressure and economic sanctions do not lose their effectiveness once exercised in an adversarial relationship.[93] CDD refinement authors thus conceive a combination of these practical measures to facilitate signalling across domains and solve the trade-off between secrecy and effectiveness.

A number of suggestions have also been presented with respect to signalling outside of the cyber domain. King Mallory observes that signalling can rely on explicit moral Manicheism through clear verbal statement that there is no middle ground or grey zone in order to persuade adversaries that any kind of hostilities, direct or indirect, will lead to retaliation.[94] Signalling of both will and capability is also possible against hybrid intrusions, especially with rapidly deployable response teams of police and Special Forces which convey to the adversary that it is not likely to achieve its interests. Other means of signalling include implicit warnings reflected in changes in postures in combination with public statements.[95] Others suggest that "acts of retorsion" including economic sanctions and diplomatic coercion/isolation are perfect signalling instruments.[96] The authors in this literature have thus come up with a broad portfolio of signalling measures across all domains.

8.3.5 Escalation Management

The combination of issues discussed in relationship to attribution, threat proportionality and signalling makes escalation management much more difficult in CDD.[97] The attribution problem injects uncertainty into the deterrence relationship because it renders unclear under which conditions the deterring actor will deem it appropriate to escalate. Challenges associated with credibility and proportionality undermine basic tenets of successful escalation management simply because of the

[90]Klimburg 2020; Geers 2015.
[91]Schneider 2019, pp. 117–118.
[92]Green and Long 2019, p. 231. Lindsay 2015, p. 58.
[93]Lindsay 2015, p. 58.
[94]Mallory 2018, pp. 10–15.
[95]Lewis 2010, p. 4.
[96]Davis 2017, p. 81.
[97]See the concluding section in "A New Look at the 21st Century Crossdomain Deterrence Initiative" 2016.

unpredictable dynamics across domains. Complexity of signalling further befuddles escalation management in practice because it is unclear whether signals are both sent and received. Accordingly, the diversity of escalation dynamics of cross domain deterrence is singled out as "a core analytic issue".[98]

An assortment of sources of instability for escalation management in CDD are discussed many of which are directly or indirectly related to issues addressed previously. First and foremost, there is no shared framework to describe and therefore manage escalation across domains.[99] Without such a framework "decision makers will have difficulty distinguishing between proportional and escalatory attacks and reprisals that cross from traditional strategic domains into these newer ones and vice versa".[100] Second, there are many sources of instability when it comes to particular measures and weapons across domains. Western superiority in conventional weapons motivates adversaries to actively seek and exploit asymmetric and diverse measures with varying kinetic and non-kinetic effects and with differing degrees of proportionality.[101] Some of the instruments and tactics operate across domains that cross potential thresholds faster than in the past.[102] In this context, the use of unmanned and semi-autonomous systems and, in the future, other AI enhanced weapon systems may be particularly destabilizing.[103] Furthermore, the nature of the cyber and space domains and the character of technologies used in these domains may generate escalation risks through first-strike instabilities.[104] This renders these domains not only inherently unstable but also implies spill over effects to other domains in CDD.[105] Consequently, the anticipated effects are sometimes difficult to gauge before their actual employment.[106] Third, proportionality perceptions of actions in particular domains vary considerably from one actor to the next.[107] For example, Russia and China tend to see the integration of military, political and economic tools in a much more holistic fashion and for this reason they are likely to appraise the conversion rate between individual domains differently. As Adamsky explains in this volume and elsewhere the Russians combine nuclear, conventional and information measures to deter continuously and across domains.[108] Dean Cheng in this volume and elsewhere, describes the Chinese understanding of deterrence to involve "political activity and

[98]Brimley 2010, p. 129.

[99]As Jervis points out, even frameworks for cyber domain escalations are rare to come by. See Jervis 2016, p. 71.

[100]Manzo 2011, p. 4.

[101]Andres 2017, p. 92; Wilner 2019, p. 9.

[102]Morgan et al. 2008, p. 168.

[103]Johnson 2020.

[104]Frear et al. 2018, p. 16.

[105]Kopec 2019, p. 125.

[106]Manzo 2015, p. 97.

[107]Manzo 2011, p. 4; Lewis 2010, p. 3.

[108]Adamsky 2015, p. 37.

psychological warfare".[109] Any combination of these three challenges may hinder attempts at successful escalation management in any particular conflict.

CDD authors once again have come up with a range of proposals how to address these issues. First and foremost, they agree that it is necessary to develop a shared framework which would encompass the expectations for escalation dynamics.[110] There are several distinct approaches to the development of a shared framework. Some scholars point to the salient function of international law. Game theorist James Morrow, for example, argues that the developments in international law can constitute a first step towards the development of such a framework. Law alleviates the uncertainties about proportionality by explicitly stating what is acceptable, what is the appropriate response as well as how these actions relate across specific domains. As a coordination mechanism, law contributes to a common understanding of proportionality. Though it is unlikely to eliminate competition, it may channel hostilities into more manageable forms.[111] In this vein, others argue that an international cyber warfare convention would improve the prospects for both deterrence by punishment and by denial "by clarifying what counts [as] an act of cyber-aggression and what level of retaliation is deemed acceptable by the international community, an ICWC would thereby enhance states' capacity to adopt and communicate an effective deterrent posture".[112] Another perspective on framework development builds upon the notion of different kinds of escalation ladders, including a "provocation framework" to elucidate thresholds in "grey-zone" competition and improve escalation management by helping "policymakers understand the value of their actions and how reciprocal and proportional responses achieve strategic effect… ".[113] Such a framework is supposed to work as an explicit "declaratory policy" to signal both commitment and expectations of proportionality.

Attempts have also been made to further develop escalation ladders to establish the logic of escalation in the context of single domains,[114] as well as in the interaction between different domains.[115]

Here, an interesting schism about whether to focus on instruments or on effects emerges. On one hand, it has been argued for cross domain frameworks to be based on the "severity of various military and non-military actions based on the full range of their anticipated effects, rather than assuming that military actions represent an escalation from non-military actions".[116] On the other hand, "cyber operations might not have the same saliency or emotional effect as conventional operations—

[109]Cheng 2017, p. 1.
[110]Manzo 2015, p. 92; Sweijs et al. 2016, p. 60.
[111]Morrow 2019, pp. 198–204.
[112]Eilstrup-Sangiovanni 2018, p. 398.
[113]Ruecking 2018, p. 15.
[114]Kopec 2019, p. 126; Szymanski 2019, p. 97.
[115]Caton 2019, pp. 28–32.
[116]Rosenberg and Tama 2019, p. 9.

even when they create the same physically destructive effects".[117] This second line of research, therefore, indicates that psychological effects vary across different instruments regardless of the physical damage these instruments cause.[118] Relatedly, it is also possible that cyber instruments are "poor tools for escalatory purposes" because of the limited cost-generation potential of offensive cyber operations".[119] This echoes the observations that actors tend to deescalate rather than escalate in the cyber domain because cyber tools enable actors to release tensions by "sub crisis management manoeuvring".[120] These practical ideas concerning the development of shared frameworks, whether alone or in some combination, thus seek to address problems associated with escalation management in CDD.

Authors working on CDD have also proposed several solutions to tackle the problems of destabilizing measures and of varying perceptions of proportionality. To deal with the former, it may be wise to avoid offensive activity with specific weapons (nuclear) and against specific targets (command and control).[121] Additionally, the vulnerable assets should be better protected. Satellites should be dispersed across broad space and have their passive and active defences improved.[122] Economic interdependence too, may have a stabilizing effect by motivating restraint in interactions. Finally, new domains tend to create mutual vulnerabilities which can incentivize prudence and caution out of fear for retaliation. Declarations of restraint as well as the developments of some basic thresholds for response are seen as time tested mechanisms.[123] This may prove particularly useful in the cyber and space domains. Other recommendations lean towards the opposite direction, with experts suggesting not to show restraint but rather to show resolve and the will to retaliate in order to establish escalation dominance up front.[124] How to combine the two contradictory approaches continues to be a pernicious problem, and requires future research and also practice to solve.[125] The ideal situation is the one in which each actor can exercise restraint but still radiate resolve.[126] These diverging recommendations imply that successful escalation management depends on the practical application in particular contexts rather than on general truths. Overall, the solutions for escalation management proposed in the refinement camp are of a predominantly practical nature. They build on, but do not

[117]Schneider 2019, p. 119.
[118]Kreps and Schneider 2019.
[119]Borghard and Lonergan 2019.
[120]Jensen and Valeriano 2019, p. 40.
[121]Manzo 2015, pp. 94–97.
[122]Harrison 2014, p. 116; MacDonald 2013, pp. 91; Morgan 2010, pp. xiv–xv.
[123]Kopec 2019, p. 126; Manzo 2015, p. 97.
[124]Jacobsen 2016, p. 7.
[125]Durkalec et al. 2018, p. 14.
[126]Frear et al. 2018.

extend, the logic of classic deterrence theory while offering a range of valuable practical insights how to effectuate CDD in today's world.

8.4 Refinement and Reinterpretation—Expansion and Reconceptualisation

The second strand in the CDD literature argues that the character of contemporary challenges requires the broadening and deepening of our understanding of deterrence. Instead of offering practical recommendations on how to effectuate CDD in light of changing strategic conditions, authors propose theoretical and conceptual additions and innovations to existing concepts of deterrence rooted in deterrence by punishment and deterrence by denial. Some authors offer additional theoretical concepts to update deterrence; other authors in effect seek to reconceptualise deterrence in light of the nature of cross-domain challenges. This stems from the recognition and conviction that new domains require new approaches. Finding incremental practical fixes simply does not suffice, so they argue. It is thought that the traditional parameters that may have allowed deterrence to work in previous times, simply no longer hold in the context of today's multipolar, connected and complex strategic environment. The greater diversity of actors that dispose of an even greater diversity of means that can successfully threaten each other in this environment either undermines deterrence or may even render it impossible.

8.4.1 Refinement of Traditional Concepts of Deterrence

Some of the additions are theoretical refinements. For instance, in order to deter across both old and new domains, concepts such as cumulative, punctuated and layered deterrence have been introduced. The concept of cumulative deterrence is based on Israel's strategic experience. Israel has defended itself against a diverse spectrum of attacks conducted by state and non-state actors over a long period of time, partly by "attacking the rival repeatedly in response to specific behaviours, over a long period of time, sometimes even disproportionally to its aggressive actions".[127] Or, as we put it in a previous publication on cross domain deterrence in the context of hybrid conflict, "cumulative deterrence conceptualises deterrence as a continuous, longer term process in which a one-off transgression does not spell failure but adversarial behaviour is shaped by the deterrer in a concerted effort."[128] Within the framework of cumulative deterrence, deterrers understand the necessity of absorbing some attacks in order to prevent others. This marks a clear departure

[127]Tor 2015, p. 112.

[128]Sweijs and Zilincik 2019, p. 23.

from a more absolutist notion encapsulated in traditional deterrence approaches aimed at deterring all attacks. The concept of cumulative deterrence may indeed be better suited to the less impactful but more frequent and ambiguous amalgamation of contemporary security threats and actors rather than to deterring the threat of a nuclear attack.[129] Another alternative is punctuated deterrence, which conveys punishment to address a series of actions and cumulative effects. The difference between cumulative and punctuated deterrence is that within the framework of cumulative deterrence, deterrers respond continuously over long time periods to single attacks, while in the case of punctuated deterrence they respond gradually over time and in a punctuated manner.[130] In the context of space deterrence, some authors have come up with the notion of layered deterrence, which includes a simultaneous combination of international norms, entanglement, retaliation, and denial of benefit which can be conducted across domains.[131]

8.4.2 Reinterpretation of Deterrence by Denial

In trying to come to terms with the nature of today's strategic challenges, authors have also sought to expand on traditional concepts of deterrence by denial and punishment, even trying to merge the two into one mechanism. Recent years have seen the introduction of notions such as offensive denial and resilient denial, punishment through stigmatization, and entanglement, as well as the substitution of dissuasion for deterrence. With respect to deterrence by denial authors have introduced the distinction between tactical and strategic denial.[132] Tactical denial refers to denying the adversary the prospect of attaining the direct impact of a particular hostile action, while strategic denial refers to denying it the political benefits that it expects to derive. While the former still aligns with traditional conceptions of deterrence by denial, the latter constitutes a significant broadening of the concept. Yet also tactical denial has been significantly expanded, most importantly by including offensive pre-emptive action. Traditional deterrence theoreticians assumed that denial is inherently tied to defensive measures, whether active or passive ones. The complexity and the opportunities presented by today's strategic landscape domains have led them to theorise ways in which offensive action can be used to deny the adversaries the means to conduct offensive action. This, again, is discussed most often in relation to the cyber domain.[133] It is also observable in strategic practice, as the US has started to pursue its persistent engagement, which is it seeks to "defend forward" by preventively denying the

[129]Rid 2012, p. 125.
[130]Kello 2017, pp. 208–209.
[131]Harrison et al. 2009, pp. 17–26.
[132]Kroenig and Pavel 2012.
[133]Sharma 2010.

adversaries their means for the conduct of hostile operations.[134] The underlying logic, however, as such holds for every other domain in which offensive means can degrade the adversaries' capabilities to fight before the actual hostile interaction takes place. It is possible to conceive of denial in more traditional domains as encapsulating pre-emptive or preventive strikes against adversarial military capabilities.[135] Similarly, Israel has relied on a strategy of cumulative attrition in order to deter its enemies from carrying out immediate attacks by denying them the capability to do so.[136] Besides, capabilities in other domains tend to rely on cyber measures to varying degrees hence the use of offensive denial may impact land, naval, air and space domains as well. Overall, this approach recognizes the fact that the adversaries' capabilities and their will to fight may be dependent upon each other and thus by denying the opportunity to use those capabilities is also likely to degrade their will to fight.

Where it comes to strategic denial, resilience is singled out as a key component.[137] Resilience is conceived as the ability to absorb the direct impact of the hostile activity in question without suffering any long-lasting impact. While originally proposed in the context of deterring terrorist attacks, recent scholarship proposes that resilience can be a strategic asset across multiple domains of competition and may be effective against both state and non-state actors.[138] Ultimately, strengthening resilience is envisaged as a cross domain effort because its objective is to prepare whole societies in a cross sectoral approach to withstand adversarial activities. Once attained, resilience then signals to the adversaries the futility of carrying out potential attacks by nullifying the potential benefits to be derived from a broad spectrum of hostile measures. To deal with the ever-increasing complexity of contemporary actors and domains, deterrence by denial has thus been conceptually stretched by including new approaches that include other types of effects.

8.4.3 Expansion of Deterrence by Punishment: Norms, Delegitimisation and Entanglement

Scholars have also proposed a broader gamut of measures encompassed under deterrence by punishment. The traditional concept is expanded to encompass deterrence through norms, delegitimisation and entanglement. Punishment through norms seeks to convince potential transgressors not to engage in certain behaviour

[134]Healey 2019.

[135]Wirtz 2018, p. 70.

[136]Efraim and Shamir 2014.

[137]See also Chap. 18 in this volume by Cees van Doorn and Theo Brinkel.

[138]Hartmann 2017; Hellman 2019.

by presenting them with the prospect of social costs.[139] It seeks to alter the cost calculus of those who do not abide by the positive standards of behaviour, while deterrence by taboos seeks to do the same to those who engage in hostilities that are generally seen as off-limits. Breaking any of these two standards risks incurring not only a domestic backlash but also the loss of international prestige and ostracisation which is detrimental to vital interests of both state and non-state actors. Deterrence by association expands on that logic. It constitutes "a political mechanism in order to 'call-out' poor behaviour and strongly condemn such actions publicly, by those with the right authority, because it acts as a clear signal to others in the community of actors what is right and wrong behaviour".[140] This extended version of deterrence by punishment is increasingly being discussed in the context of deterrence in new domains and in relation to both state and non-state actors but is equally applicable to any other domain.[141]

A second alternative strategy, delegitimisation, is loosely based on the logic of punishment as it aims "to raise the costs of participating in terrorism by challenging the normative, religious, and socio-political rationales individuals rely upon when participating in violence".[142] Authors in this strand also argue that this approach allows for the classification of both particular instruments and particular targets as unacceptable. The traditional deterrence literature also addressed this, but it may be even more relevant in the cross-domain context, because the new context makes it possible to channel the conflict into more manageable domains. In some cases, such as with nuclear threats, the focus on the stigmatisation of particular weapons may be more effective. For instance, the stigmatisation of biological, chemical and nuclear weapons which has developed gradually during the last century, was closely connected to the destructive nature of these weapons.[143] This logic may be applicable to space deterrence too if it is accepted "that encouraging behavioural norms regarding the peaceful use of space—and thereby increasing the political stigma of using weapons in space—is desirable…" because "even relatively weak political stigmas can deter attacks in space for players with something to lose."[144] It is plausible, for example, that attacks against satellites should be discouraged by the development of an appropriate normative framework.[145] In other cases, such as the cyber domain, targets rather than instruments may warrant more attention.[146] Deterrence through norms may thus adhere to the original logic of deterrence by violent punishment but certainly stretches its scope. It relies on a broader concept of

[139]Ryan 2017.
[140]Ryan 2017, p. 335.
[141]Nye 2017, p. 62.
[142]Wilner 2011, p. 27.
[143]Shamai 2020.
[144]Triezenberg 2017, p. 2.
[145]Lewis 2013, p. 79.
[146]Nye 2017, p. 61.

punishment by including the social and psychological costs in order to deter actions from engaging in certain behaviour.

A third way in which traditional concepts of punishment are stretched revolves around entanglement.[147] Entanglement relies on fostering interdependence between actors and contributes to deterrence success by shaping the cost calculus of potential adversaries, as suggested by Joseph Nye. The assumption is that actors entangled in mutually dependency relationships will refrain from launching attacks because they themselves will incur costs too. It works by persuading potential adversaries that the continuation of the status quo is in their own interest, hence they should be reluctant to launch an attack in the first place.[148] The logic of entanglement, in the cyber domain and beyond, works by "adding more factors into the deterrence cost calculus— economic, political and diplomatic, for instance— then an adversary can be entangled…since they would have to suffer the consequences in other areas of their relations."[149] Essentially, entanglement operates by "mutual establishment and recognition as well as perception management of benefits both in the present and over time".[150] Or, to put it another way, entanglement works by persuading the relevant actors that they are "stakeholders in cyberspace" which should motivate them to exercise restraint in offensive behaviour.[151] Due to their mutual interdependence, this kind of deterrence is most often discussed in the context of the overall Sino-American relationship.[152] But that logic may also apply to the space domain because attacks against commercial satellites can impede international trade and finance.[153] Deterrence through norms and deterrence through entanglement are thus seen as necessary expansions in today's globally connected world. The theoretical innovations offered expand the scope of deterrence by taking a more holistic view of the overall incentive structure of potential targets of deterrence and including less tangible factors such as identity and social belief systems into consideration as well as non-military dimensions to affect the cost-benefit calculus of potential adversaries.

8.4.4 From Deterrence to Dissuasion

Finally, authors argue that deterrence of contemporary threats requires expanding classical concepts of deterrence not just in terms of the ways and means but also in its very nature. Taking stock of the theoretical additions and innovations to address

[147]Brantly 2018a.
[148]Nye 2017, p. 58.
[149]Ryan 2017, pp. 336–337.
[150]Brantly 2018b.
[151]Jasper 2015, p. 67.
[152]Pontbriand 2019.
[153]Rao et al. 2017, p. 55.

today's challenges, they argue that our common understanding of deterrence needs to be reconceptualised or rather that fundamental features that were mentioned in the classic deterrence literature require much greater emphasis. They argue that deterrence will have to focus both on persuasion and dissuasion and include both positive and negative incentives in order to prevent adversaries from engaging in undesired behaviour. Dissuasion, for example, can be seen within a broader approach to deterrence as a form that includes both threats and inducements but also "reassurances and benefits that make a world without aggression more attractive".[154] The advantage of dissuasion is that it can be pursued "through international institutions, treaties, economic sanctions, raising reputation costs, soft balancing, and diplomatic engagement".[155] Dissuasion, a subset of what can be termed "compliance seeking efforts", is supposed to include not only negative but also positive measures and it can work both by increasing the attractiveness of particular options and by decreasing the desirability of others.[156] While these ruminations may seem to be a classic case of concept creep, it is worth noting that they can also be considered a rediscovery of insights already coined by classical deterrence theorists. After all, in the early 1960s Glenn Snyder defined deterrence as "the power to dissuade" which is done by "the implicit or explicit threat of applying some sanction if the forbidden act is performed, or by the promise of a reward if the act is not performed" so that it constitutes "a process of influencing the enemy's intentions, whatever the circumstances".[157]

8.5 Conclusion

Strategic concepts emerge in particular strategic contexts to deal with specific challenges in a given period. Some strategic concepts wither away once the strategic environment evolves, others persist but are adapted. Our review of the CDD literature finds a thriving scholarly and professional debate about the use and utility of deterrence in the context of today's cross domain challenges. Our review reveals significant continuities but also significant changes in the insights offered by the CDD literature compared to the preceding waves in the deterrence literature. Deterrence has been cross domain in character since its early beginnings, prompting some to pose the question whether CDD is nothing more than old wine being served in new bottles. Accordingly, Gartzke and Lindsay start their 2019 edited volume by asking "whether CDD provides any additional analytical traction beyond classical notions of deterrence…" because "deterrence in practice has always dealt with …different military services with different nuclear, conventional, and

[154]Mazarr 2018, p. 5; see also Nye 2017.
[155]Paul 2018, p. 35.
[156]De Spiegeleire et al. 2020.
[157]Snyder 1961, pp. 106–107.

unconventional weapons, together with various diplomatic, economic, and cultural instruments of national power."[158] The continuities with traditional deterrence literature are indeed considerable: traditional concepts of deterrence by punishment and denial are still part and parcel of the strategic lexicon; the literature keeps returning to favouring conditions of successful deterrence including the communication of credible threats of cost imposition which is rooted in robust capabilities and will. At the same time, there is certainly no stasis in the CDD literature. As demonstrated in the review offered in this chapter, significant developments can be found both in terms of practical application and theoretical innovation. This speaks to the idea that CDD is more than just old wine being served in new bottles. Overall, our review warrants three main conclusions.

First, authors have spent considerable effort on the practical application of key tenets of traditional deterrence theory in the context of contemporary strategic challenges. This has resulted in an assortment of innovative ideas predominantly focused on practical measures and opportunities to deal with challenges related to attribution, threat credibility and proportionality, signalling and escalation management.

Second, authors have also come up with a number of theoretical advancements. In addressing today's strategic challenges, they have refined and expanded on traditional concepts of deterrence by stressing that successful deterrence should be envisaged as a continuous process, by usefully differentiating in deterrence by denial between tactical and strategic impacts, by adding resilience to the other side of the denial coin; by incorporating social costs in the deterrence by punishment equation; and by complementing the traditional dominant focus on negative payoff structures with attention to the role played by positive incentive structures.

Third, in light of these refinements and expansions of the concept deterrence, the question is warranted whether this enlightened notion of deterrence is still in fact about the act of *deterring* an opponent or whether it in effect constitutes a reconceptualisation of the essence of deterrence by making it about *dissuading* but also *persuading* instead of *deterring*. After all, this expanded concept of dissuasion implies a more diverse range of instruments, both military and non-military, which can be used both as a stick and a carrot, both to compel and to deter, both to persuade and to dissuade, which brings it back to the broader coercive diplomacy literature from which it originally emerged.

Our own assessment finally is that dissuasion, rather than being akin to deterrence, is more fitting as an overarching concept which encompasses the various means and ways by which one can dissuade the adversary to abstain from the action.[159] As such it includes both positive inducements and negative threats. Dissuasion can thus work as an umbrella term for deterrence by denial and punishment, norms, entanglement, resilience and assurance. Given the salience of the

[158]Lindsay and Gartzke 2019a, pp. 3–4. They eventually find CDD to be more than just old wine because it emphasises the importance of means much more than was customary in the traditional deterrence writings. See Lindsay and Gartzke 2019b, pp. 335–340.

[159]We would like to thank Stephan De Spiegeleire for his contribution to the development of this idea and for extended discussions on this topic. See also De Spiegeleire et al. 2020.

hostilities conducted below the legal thresholds of international law as well as the inability or reluctance of states to respond to varied intrusion across all domains. This broader concept of dissuasion may be more appropriate in the context of the strategic challenges in today's world.

References

Ablon L, Bogart A (2017) Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. RAND Corporation, Santa Monica

Adamsky D (2015) Cross-Domain Coercion: The Current Russian Art of Strategy. Security Studies Center, Paris

Andres R (2017) Cyber Grey Space Deterrence. PRISM 7:91–98

Bahney B W, Pearl J, Markey M (2019) Antisatellite Weapons and the Growing Instability of Deterrence. In: Lindsay J R, Gartzke E A (eds) Cross-Domain Deterrence: Strategy in an Era. Oxford University Press, Oxford, 121–143

Black J (2018) Combined Operations: A Global History of Amphibious and Airborne Warfare. Rowman and Littlefield, London

Blagden D (2020) Deterring Cyber Coercion: The Exaggerated Problem of Attribution. Survival 62:131–148

Borghard E D, Lonergan SW (2019) Cyber Operations as Imperfect Tools of Escalation. Strategic Studies Quarterly 13:122–145

Brantly A (2018a) Back to Reality: Cross Domain Deterrence and Cyberspace. Virginia Tech, Boston

Brantly A (2018b) Conceptualizing Cyber Deterrence by Entanglement. Social Science Research Network, Rochester, NY

Brimley S (2010) Promoting Security in Common Domains. The Washington Quarterly 33:119–132

Buckley C H (2018) Building 'Space' into Multi-Domain Deterrence Strategy. http://www.airpowerstrategy.com/2018/12/01/space-deterrence/. Accessed 30 May 2020

Caton J L (2019) The Army Role in Achieving Deterrence in Cyberspace. Strategic Studies Institute, Carlisle

Cheng D (2017) Evolving Chinese Thinking About Deterrence: The Nuclear Dimension. The Heritage Foundation, Washington

Cioffi-Revilla C (1999) Origins and Age of Deterrence: Comparative Research on Old World and New World Systems. Cross-Cultural Research 33:239–264

Cormac R, Aldrich R (2018) Grey Is the New Black: Covert Action and Implausible Deniability. International Affairs 94:477–494

Cullen P, Wegge N (2019) Countering Hybrid Warfare. Development, Concepts and Doctrine Centre, Shrivenham

Davis J E (2017) Remarks by Jonathan E. Davis. Proceedings of the ASIL Annual Meeting 110:78–81

Dawkins JC (2009) Rising Dragon: Deterring China in 2035. Defense Technical Information Center, Fort Belvoir, VA

De Spiegeleire S, Holynska K, Batoh Y, Sweijs T (2020) Reimagining Deterrence: Towards Strategic (Dis)Suasion Design. The Hague Centre for Strategic Studies, The Hague

Denning D E (2015) Rethinking the Cyber Domain and Deterrence. Joint Force Quarterly 7:8–15

Durkalec J, Paige G, Shykov O (2018) 5th Annual LLNL Deterrence Workshop Multi-Domain Strategic Competition: Rewards and Risks. Lawrence Livermore National Laboratory, Livermore

Efraim I, Shamir E (2014) Mowing the Grass: Israel's Strategy for Protracted Intractable Conflict. Journal of Strategic Studies 37:65–90
Eilstrup-Sangiovanni M (2018) Why the World Needs an International Cyberwar Convention. Philosophy and Technology 31:379–407
Frear T, Kulesza L, Raynova D (2018) Russia and NATO: How to Overcome Deterrence Instability? https://www.europeanleadershipnetwork.org/report/russia-and-nato-how-to-overcome-deterrence-instability/. Accessed 30 May 2020
Fridman O (2018) Russian 'Hybrid Warfare': Resurgence and Politicization. Oxford University Press, Oxford
Geers K (2015) Cyber War in Perspective: Russian Aggression against Ukraine. NATO CCD COE, Tallinn
George A, Smoke R (1974) Deterrence in American Foreign Policy. Columbia University Press, New York
Green BR, Long AG (2019) Signalling with Secrets: Evidence on Soviet Perception and Counterforce Developments in the Late Cold War. In: Lindsay JR, Gartzke EA (eds) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press, Oxford, 205–233
Harrison R (2014) The Role of Space in Deterrence. In: Schrogl K-U et al. (eds) Handbook of Space Security. Springer, Prague, 113–130
Harrison R, Jackson D, Shackelford C (2009) Space Deterrence: The Delicate Balance of Risk. Space and Defense 3: 1-30
Hartmann U (2017) The Evolution of the Hybrid Threat, and Resilience as a Countermeasure. Center for Security Studies, Zurich
Hayes R E, Alberts DS (2003) Power to the Edge: Command and Control in the Information Age. Department of Defense, Washington
Healey J (2018) Not the Cyber Deterrence the United States Wants. https://www.cfr.org/blog/not-cyber-deterrence-united-states-wants. Accessed 30 May 2020
Healey J (2019) The Implications of Persistent (and Permanent) Engagement in Cyberspace Journal of Cybersecurity. Journal of Cybersecurity 5:1–15
Hellman A (2019) How Has European Geostrategic Thinking towards Russia Shifted since 2014? https://www.europeanleadershipnetwork.org/policy-brief/how-has-european-geostrategic-thinking-towards-russia-shifted-since-2014/. Accessed 30 May 2020
Hoffman, F G (2018) Examining Complex Forms of Conflict: Grey Zone and Hybrid Challenges. PRISM 7:30–47
Iasiello E (2014) Is Cyber Deterrence an Illusory Course of Action? Journal of Strategic Security 7:54–67
Innes M A (2012) Making Sense of Proxy Wars: States, Surrogates & the Use of Force. Potomac Books, Lincoln
Jackson N J (2019) Deterrence, Resilience and Hybrid Wars: The Case of Canada and NATO. Journal of Military and Strategic Studies 19:104–25
Jacobsen E (2016) 3rd Annual Cross-Domain Deterrence Seminar: Towards Integrated Strategic Deterrence. Lawrence Livermore National Laboratory, Livermore
Jasper S (2015) Deterring Malicious Behaviour in Cyberspace. Strategic Studies Quarterly 9:60–85
Jensen B, Valeriano B (2019) What Do We Know About Cyber Escalation? Observations from Simulations and Surveys. Scowcroft Center for Strategy and Security, Washington
Jervis R (2016) Some Thoughts on Deterrence in the Cyber Era. Journal of Information Warfare 15:66–73
Johnson D E (2018) Shared Problems - The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle. RAND Corporation, Santa Monica
Johnson J S (2020) Artificial Intelligence: A Threat to Strategic Stability. Strategic Studies Quarterly 14:16–39
Juarez A (2016) 2015 Cross-Domain Deterrence Seminar Summary Report. Lawrence Livermore National Laboratory, Livermore
Kahn H (1965) On Escalation: Metaphors and Scenarios. Praeger, Santa Barbara

Kello L (2017) The Virtual Weapon and International Order. Yale University Press, Yale.
Kennan G (1948) Policy Planning Staff Memorandum. http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm. Accessed 30 May 2020
Klimburg A (2017) The Darkening Web: The War for Cyberspace. Penguin Books, New York
Klimburg A (2020) Mixed Signals. Survival 62:107–130
Knopf J W (2010) The Fourth Wave in Deterrence Research. Contemporary Security Policy 31:1–33
Kopec R (2019) Space Deterrence: In Search of a 'Magical Formula. Space Policy 47:121–129
Kreps S, Schneider J (2019) Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics. Journal of Cybersecurity 5:1–11
Kroenig M, Pavel B (2012) How to Deter Terrorism. The Washington Quarterly 35:21–36
Lambakis S (2019) A Guide for Thinking about Space Deterrence and China, Comparative Strategy 38:497–553
Lehman R (2019) Simplicity and Complexity in the Nth Nuclear Era. In: Lindsay JR, Gartzke EA (eds) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press, Oxford, 66-91
Lewis J A (2010) Cross-Domain Deterrence and Credible Threats. Center for Strategic and International Studies, Washington
Lewis JA (2013) Reconsidering Deterrence for Space and Cyberspace. In: Krepon M, Thompson J (eds) Anti-Satellite Weapons, Deterrence and Sino-American Space Relations. The Stimson Center, Washington, 61–80
Lindsay J R (2015) Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack. Journal of Cybersecurity 1:53–67
Lindsay J R, Gartzke E A (2016) Draft: Cross-Domain Deterrence as a Practical Problem and a Theoretical Concept. In: Lindsay JR, Gartzke EA (eds) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press, Oxford, 1–35
Lindsay J R, Gartzke E A (2019a) Introduction: Cross-Domain Deterrence, From Practice to Theory. In: Lindsay J R, Gartzke E A (eds) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press, Oxford, 1–26
Lindsay J R, Gartzke E A (2019b) Conclusion: The Analytic Potential of Cross-Domain Deterrence. In: Lindsay J R, Gartzke E A (eds) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press, Oxford, 335–371
Long A (2008) Deterrence – From Cold War to Long War. RAND Corporation, Santa Monica
Lonsdale D J (2018) Warfighting for Cyber Deterrence: A Strategic and Moral Imperative. Philosophy & Technology 31:409–429
Luttwak E (2002) Strategy: The Logic of War and Peace. The Belknap Press of Harvard University Press, London
MacDonald B W (2013) Deterrence and Crisis Stability in Space and Cyberspace. In: Krepon M, Thompson J (eds) Anti-Satellite Weapons, Deterrence and Sino-American Space Relations. The Stimson Center, Washington, 81–100
Mallory K (2018) New Challenges in Cross-Domain Deterrence. RAND Corporation, Santa Monica
Mandel R (2017) Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks. Georgetown University Press, Washington
Manzo V (2011) Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit? https://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-272.pdf. Accessed 30 May 2020
Manzo V (2015) After the First Shots Managing Escalation in Northeast Asia. Joint Force Quarterly 77:91–100
Mazarr M J (2018) Understanding Deterrence. Santa Monica, RAND Corporation
Mercer J (1996) Reputation and International Politics. Cornell University Press, Ithaca
Milevski L (2019) Grand Strategy Is Attrition. Strategic Studies Institute, Carlisle
Morgan F E (2010) Deterrence and First-Strike Stability in Space: A Preliminary Assessment. RAND Corporation, Santa Monica

Morgan F E, Mueller K P, Medeiros E S, Pollpeter K L, Cliff R (2008) Dangerous Thresholds: Managing Escalation in the 21st Century. RAND Corporation, Santa Monica
Morris LJ, Mazarr MJ, Hornung JW, Pezard S, Binnendijk A, Kepe M (2019) Gaining competitive advantage in the gray zone. RAND Corporation, Santa Monica
Morrow J D (2019) International Law and the Common Knowledge Requirements of Cross-Domain Deterrence. In: Lindsay J R, Gartzke E A (eds) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press, Oxford, 187–204
Naroll R (1974) Military Deterrence in History: A Pilot Cross-Historical Survey. State University of New York Press, Albany
Nye J S (2017) Deterrence and Dissuasion in Cyberspace. International Security 41:44–71
Office of the Director of National Intelligence (2018) A Guide to Cyber Attribution. https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf. Accessed 30 May 2020
Paul T V (2018) Reimagining Deterrence: New Security Threats and Challenges to the Deterrence Paradigm. In: Wasser et al. (eds) Comprehensive Deterrence Forum. RAND Corporation, Santa Monica, 31–36
Pontbriand K (2019) Cyber Entanglement: A Framework for the Study of U.S.–China Relations. In: Cruz T, Simoes P (eds) Proceedings of the 18th European Conference on Cyber Warfare and Security ECCWS 2019. ACPI, Coimbra, 702–709
Press D G (2005) The Credibility of Power: Assessing Threats During the 'Appeasement' Crises of the 1930s. International Security 29:136–169
Rao V R, Gopalakrishnan V, Abhijeet K, Sadeh E (2017) International Space Governance: Challenges for the Global Space Community. In: Rao V R, Gopalakrishnan V, Abhijeet K, Sadeh E (eds) Recent Developments in Space Law. Springer, Singapore, 43–59
Rid T (2012) Deterrence beyond the State: The Israeli Experience. Contemporary Security Policy 33:124-147
Robinson L, Helmus TC, Cohen RS, Alireza N, Radin A, Magnuson M, Migacheva K (2018) Modern Political Warfare: Current Practices and Possible Responses. RAND Corporation, Santa Monica
Romanosky S, Goldman Z (2016) Cyber Collateral Damage. Procedia Computer Science 95:10–17
Rosenberg E, Tama J (2019) Strengthening the Economic Arsenal: Bolstering the Deterrent and Signalling Effects of Sanctions. Center for New American Security, Washington
Rovner J (2019) Can the United States Deter Election Meddling? https://warontherocks.com/2019/11/can-the-united-states-deter-election-meddling. Accessed 30 May 2020
Ruecking D W (2018) Winning in the Grey Zone: A Provocation Framework Approach. US Naval War College, Newport
Ryan N (2017) Five Kinds of Cyber Deterrence. Philosophy & Technology 31:331–338
Sayler K (2015) A World of Proliferated Drones: A Technology Primer. Center for New American Security, Washington
Schelling T C (1966) Arms and Influence. Yale University Press, New Haven
Schneider J (2019) Deterrence in and through Cyberspace. In: Lindsay J R, Gartzke E A (eds) Cross-Domain Deterrence: Strategy in an Era of Complexity. Oxford University Press, Oxford, 95–120
Scouras J, Smyth E, Mahnken T (2017) Cross-Domain Deterrence in US–China Strategy. Johns Hopkins Applied Physics Laboratory, Laurel
Shamai P (2020) What's in a Name? Deterrence and the Stigmatisation of WMD. In: Filippidou A (ed) Deterrence: Concepts and Approaches for Current and Emerging Threats. Springer, Basel, 77–96
Sharma A (2010) Cyber Wars: A Paradigm Shift from Means to Ends. Strategic Analysis 34:62–73
Sheppard L, Conklin M (2019) Warning for the Grey Zone. Center for Strategic and International Studies, Washington
Smeets M (2017) A Matter of Time: On the Transitory Nature of Cyberweapons. Journal of Strategic Studies 41:6–32

Smeets M, Lin H S (2018) Offensive Cyber Capabilities: To What Ends? In: Minarik T, Jakschis R, Lindstrom S (eds) 10th International Conference on Cyber Conflict CyCon X: Maximising Effects. NATO CCD COE, Tallinn, 55–72
Snyder G H (1961) Deterrence and Defence: Toward a Theory of National Security. Princeton University Press, Princeton
Stoker D, Whiteside C (2020) Blurred Lines: Grey-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking. Naval War College Review 73:1–37
Stone J (2013) Cyber War Will Take Place! Journal of Strategic Studies 36:101–108
Suzuki K (2018) A Japanese Perspective on Space Deterrence and the Role of the Japan-US Alliance in Sino-US Escalation Management. In: Wright N (ed) Outer Space; Earthly Escalation? Chinese Perspectives on Space Operations and Escalation. Department of Defense, Washington, 44–48
Sweijs T, Bekkers B, De Spiegeleire S, Oosterveld W (2016) Back to the Brink: Escalation and Interstate Crisis. The Hague Centre for Strategic Studies, The Hague
Sweijs T, Zilincik S (2019) Cross Domain Deterrence and Hybrid Conflict. The Hague Centre for Strategic Studies, The Hague
Szymanski P (2019) Techniques for Great Power Space War. Strategic Studies Quarterly 13: 78–104
Tor U (2015) Cumulative Deterrence' as a New Paradigm for Cyber Deterrence. Journal of Strategic Studies 40:92–117
Treverton G F (2018) The Intelligence Challenges of Hybrid Threats: Focus on Cyber and Virtual Realm. Center for Asymmetric Threat Studies, Stockholm
Triezenberg B L (2017) Deterring Space War - An Exploratory Analysis Incorporating Prospect Theory into a Game Theoretic Model of Space Warfare. RAND Corporation, Santa Monica
Trujillo C (2014) The Limits of Cyberspace Deterrence. Joint Force Quarterly 75:44–52
University of California (2016) A New Look at the Cross-domain Deterrence Initiative https://deterrence.ucsd.edu/_files/CDDI2-Workshop-Summary-080916.pdf. Accessed 30 May 2020
Valeriano B, Maness R C (2015) Cyber War versus Cyber Realities. Oxford University Press, Oxford
Vince R J (2015) Cross-Domain Deterrence Seminar Summary Notes. Center for Global Security Research, Livermore
Wall M (2019) North Korea's Short-Range Missile Test Spotted from Space. https://www.space.com/north-korea-missile-test-satellite-photo.html. Accessed 30 May 2020
Waxman M C (2013) Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions. International Law Studies 89:109–122
Wilner A (2011) Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism. The Journal of Strategic Studies 34:3–37
Wilner A (2019) US Cyber Deterrence: Practice Guiding Theory. Journal of Strategic Studies 42:245–280
Wirtz J J (2018) How Does Nuclear Deterrence Differ from Conventional Deterrence? Strategic Studies Quarterly 12:58–75

Wright T (2019) Democrats Must Act Now to Deter Foreign Interference in the 2020 Election. https://www.theatlantic.com/ideas/archive/2019/10/democrats-can-stop-political-interference-2020/599329/. Accessed 30 May 2020

Wuest C (2018) Multi-Domain Deterrence Table Top Exercise Summary. Lawrence Livermore National Laboratory, Livermore

Yee V, Yonette J, Magra I (2019) Iran Says It Has Seized Another Oil Tanker in Persian Gulf. https://www.nytimes.com/2019/08/04/world/middleeast/iran-oil-tanker-persian-gulf.htm. Accessed 30 May 2020

Dr. Tim Sweijs is the Director of Research at The Hague Centre for Strategic Studies and a Research Fellow at the Netherlands Defence Academy. He is the initiator, creator and author of numerous studies, methodologies, and tools for horizon scanning, early warning, conflict analysis, national security risk assessment, and strategy and capability development. He serves as an Adviser Technology, Conflict and National Interest to the UK Government's Stabilisation Unit. Tim holds degrees in War Studies (Ph.D., M.A.), International Relations (M.sc.) and Philosophy (B.A.) from King's College, London and the University of Amsterdam.

Samuel Zilincik is a doctoral student of Security and Strategic studies at Masaryk University and a teaching assistant at the University of Defence in the Czech Republic. He also has conducted internships at the Hague Centre for Strategic Studies in the Netherlands), at the Centre for Security and Prevention in the Czech Republic, and at the Strategic Policy Institute in Slovakia.